Dr.WEB®
с 1992 года

AVTRADE

Правила ПДн-гигиены для бизнеса любого размера

Собираете, храните, иным образом обрабатываете персональные данные своих сотрудников или клиентов?

Значит, вы являетесь оператором персональных данных (ПДн).

Лишь несколько примеров

- **Интернет-магазин**, программно обрабатывающий заказы клиентов и хранящий на компьютерах персональные данные клиентов.
- **Ресторан**, который выдает клиентам карты лояльности после заполнения анкеты и хранит эти персональные данные.
- **Пункт химчистки**, который собирает от клиентов их Ф.И.О. и телефонные номера, чтобы перезвонить или отправить СМС с сообщением о готовности заказа.
- **Агрегатор рассылок** (например, со скидками), для подписки на которые нужно предоставить персональные данные.
- **Индивидуальный предприниматель**, который использует труд наемных работников.
- **Медучреждение**, принимающее согласие на медицинское вмешательство или отказ от него, хранящее медицинские карты, истории болезни, рецепты и т. д.
- **Управляющая компания,** которая получает от жильцов персональные данные для оказания услуг, в том числе для формирования платежных документов.
- **Интернет-форум** или онлайн-клуб по интересам, где требуется регистрация с предоставлением персональных данных.
- Любое **образовательное учреждение**.

Если собираемые у людей персональные данные хранятся в базах данных или иным образом обрабатываются с помощью информационных технологий и технических средств (например, на компьютерах), это считается **ИСПДн** (*информационной системой по обработке персональных данных*).

Хозяйствующие субъекты не живут в изолированной среде, а «общаются» в электронном виде с информационными системами других компаний, а также с государственными информационными системами (ГИС).

Примеры ГИС: АИС «Налог» (ФНС России), «ЦБСД» (Росстат), «ГосСОПКА (ФСО России), ЕИИС «Соцстрах», ИС «Меркурий».

Согласно Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», **ЛЮБАЯ ГИС** является объектом критической информационной структуры (**КИИ**), но важно помнить, что далеко не каждый объект КИИ является частью ГИС. Объекты КИИ — это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ.

К субъектам КИИ законом отнесены не только государственные органы и учреждения, но и (внимание!) — российские юридические лица и ИП, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, **функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности**. Более того, российские юридические лица и ИП, которые обеспечивают лишь взаимодействие указанных систем или сетей, — тоже являются субъектами КИИ!

За нарушения при обработке ПДн в КИИ, неправомерный доступ к ПДн в КИИ, нарушения правил эксплуатации КИИ, а также за вирусные инциденты в этих системах — причем даже если существенного ущерба в результате инцидента не было! — предусмотрена **уголовная** ответственность.

> В случае возникновения инцидентов неправомерного воздействия на КИИ должностные лица организаций, чьи действия или бездействие привели к вирусозависимым компьютерным инцидентам (ВКИ) в КИИ, могут понести наказание, вплоть до лишения свободы на срок **от двух до десяти лет** с лишением права занимать определенные должности или заниматься определенной деятельностью (ст. 274.1 УК РФ). Аналогичные меры предусмотрены законодательством Российской Федерации и в области защиты других видов информации с ограниченным доступом.

Какие нарушения в работе ИС могут произойти в результате ВКИ

- **Хищение или порча данных** — сотрудниками, роботами и компьютерными устройствами, принадлежащими организации/ИП, или с BYOD-устройств сотрудников, или с устройств третьих лиц, которые используют недостатки в существующей системе защиты данных.
- **Нарушения в работе (Г)ИС**, вызванные ВКИ с подключенных к системам устройств; утечки данных; незаконный доступ к системам с устройств организаций/ИП или их сотрудников.
- **Распространение ВПО** с устройств организации/ИП и заражение ими ИС, информационных сред и устройств других лиц.
- **Ненадлежащая идентификация** участников коммуникаций в бизнес-процессах организации/ИП, в результате чего возможны факты мошенничества.

Основные причины — **бездействие или халатность** в обеспечении защиты информации в ИС, в том числе персональных данных в ИСПДн.

Важно иметь в виду: ответственность предусмотрена законодательством РФ не только для руководителей организаций/ИП, но и соответствующих должностных лиц, сотрудников с определенным функционалом!

Соблюдение правил обработки ИСПДн контролирует Роскомнадзор.

Для этого он наделен правом проводить плановые (документарные) и внеплановые (выездные) проверки.

Что может послужить причиной внеплановой проверки?

Например, жалоба вашего клиента или сотрудника на нарушения в сфере обработки ПДн. Или решение уполномоченного органа о проведении плановой проверки, о чем вас уведомят не позднее чем за 3 рабочих дня до даты начала ее проведения (письмом по почте, в виде электронного документа, подписанного ЭП).

Административные (ст. 13.11 КоАП РФ) санкции за различные нарушения требований законодательства РФ в сфере обработки ПДн — предупреждение или штраф (при отсутствии признаков уголовно наказуемых деяний).

Предупреждение	Штрафы	Запрет обработки ПДн
	За одно (!) нарушение: 1) организации — до 75 000 рублей 2) должностные лица — до 10 000 рублей 3) ИП — до 20 000 рублей	До устранения нарушения.

Как бизнесу обеспечить выполнение требований регуляторов по обработке ПДн

1. Устройства компании должны быть защищены, в том числе **антивирусом**.
2. Антивирус должен быть **сертифицирован**.
3. Государственные ИС, в том числе ИСПДн и иные объекты КИИ, должны быть защищена **российским антивирусом**.

Для выполнения требований регуляторов по антивирусной защите компьютерных устройств используйте **Dr.Web Enterprise Security Suite**.

Продукты комплекса имеют сертификаты ФСТЭК России и Минобороны России (ИТ.САВЗ.А2.ПЗ, ИТ.САВЗ.Б2.ПЗ, ИТ.САВЗ.В2.ПЗ, ИТ.САВЗ.Г2.ПЗ), ФСБ России (классов А2, Б2, В2, Г2, Д2 для защиты государственной тайны).

Это позволяет выполнять требования норм регуляторов по защите ИСПДн до 1-го уровня защищенности включительно, ГИС до 1-го класса защищенности включительно, систем обработки сведений, содержащих государственную тайну, любых объектов КИИ вплоть до высшей категории.

Dr.Web — российский сертифицированный антивирус

Программы Dr.Web в Едином реестре российских программ	Dr.Web сертифицирован ФСТЭК России, ФСБ России, Минобороны России	Dr.Web совместим с российскими ОС	Круглосуточная техподдержка в России